BY ORDER OF THE COMMANDER
19TH AIRLIFT WING

LITTLE ROCK AIR FORCE BASE
INSTRUCTION 33-104

6 JUNE 2014

Communications and Information

CONTINGENCY AND BUSINESS CONTINUITY PLAN FOR LITTLE ROCK ENCLAVE

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at **www.e-Publishing.af.mil.**

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: 19 CS/SCOO

Certified by: 19 CS/CC
(Lt Col. Jason P. Mobley)
Pages: 29

This instruction implements AFPD 33-1, *Cyberspace Support.* It applies to 19th Airlift Wing (19 AW) and those organizations assigned or attached to Little Rock AFB, AR who are provisioned in the Air Force Network domain and use the base enclave. This instruction addresses the elements necessary to ensure continuity of service for critical business functions during various emergencies. It also establishes procedures to recover the information system following a disruption. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional chain of command.

1. General:

1.1. The Department of Defense (DOD) defines an Information System (IS) as: a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. It includes information system applications (AIS), enclaves, outsourced information technology (IT) based processes, and platform IT interconnections. This term IS is used interchangeably as defined above by DoD.

2. Purpose and Objectives

2.1. The purpose of this Contingency and Business Continuity Plan (CBCP) is to establish procedures to recover the Little Rock AFB enclave identified as C-E.N.G.C.Scott.LittleRock.

2.2. The following objectives have been established for this plan:

2.2.1. Maximize the effectiveness of contingency operations through an established plan that consists of the three phases. The first phase is Notification/Activation phase. During this portion of the plan damage is detected and accessed and a determination is made whether or not to activate the plan. The second phase is Recovery phase and during this period of the plan operations are restored a temporary or alternate IS. Also actions are taken to recover damage which occurred to the original system. The final phase is the Reconstitution phase. During this portion of the plan IS processing capabilities are restored to normal operations.

2.2.2. Identify the activities, resources, and procedures needed to carry out IS processing requirements during prolonged interruptions to normal operations.

2.2.3. Assign responsibilities to designated personnel and provide guidance for recovering C-E.N.G.C.Scott.LittleRock during prolonged periods of interruptions to normal operations.

2.2.4. Ensure coordination with other staff who will participate in the contingency planning strategies. Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

3. Applicability

3.1. This CBCP applies to the functions, operations and resources necessary to restore and resume operations as it is currently installed and/or used. Maintenance responsibilities associated with C-E.N.G.C.Scott.LittleRock recovery procedures and as they apply to this CBCP are identified under Section 2.3, Responsibilities.

3.2. The Core Business functions and associated systems aligned with this CBCP are identified in Table 1 below:

Table 1. Core Business Functions and Associated Systems

CORE BUSINESS FUNCTION AND ASSOCIATED SYSTEM	
Communications	Active Directory, Dynamic Host Configuration (DHCP),Host Base Security System (HBSS), Automated Security Incident Measurement System (ASIMS), Proxy, Exchange, Boundary, Domain Name System (DNS)
Logistics	Global Air Transportation Execution System (GATES), Fuels
Weather	Joint Environmental Toolset (JET)
Intel	123 Intelligence mission
C-130 JMATS	Graduate Training Integration Management System (GTIMS)
Medical	Armed Forces Health Longitudinal Technology Application (AHLTA), Digital Dental Radiography Solution (DDRS), Integrated Clinical Database (ICDB), Composite Health Care System (CHCS), Picture Archiving and Communication System (PACS), (AGFA), Defense Medical Logistics Standard Support (DMLSS), General Sales License (GSL)
Contracting	File Server
Civil Engineering	ACES-FD, GEOBASE
29 WPS	PEX, File Server
Aircraft Maintenance	GO81
Aircraft Operations	Mission Planning System (MPS)

4. Scope

4.1. Planning Principles

4.1.1. Various scenarios were considered to form a basis for the plan, and multiple assumptions were made. The C-E.N.GC.Scott.LittleRock IS must indicate how the business requirement will be fulfilled if the IS is down due to an extraordinary event. The applicability of the plan is predicated on these key principles.

4.1.2. The IS is inaccessible and fails to meet minimum production requirements.

4.1.3. An alternate site and/or alternate process must be developed and available for implementation if required.

4.1.4. C-E.N.GC.Scott.LittleRock will use the alternate site building and IS resources to recover functionality during an emergency situation that prevents access to the original facility.

4.1.5. The designated computer system at the alternate site has been configured to begin processing information.

4.1.6. The alternate site will be used to continue recovery and processing throughout the period of disruption, until the return to normal operations.

4.2. Assumptions/Constraints

4.2.1. Based on these principles, the following assumptions/constraints were used in developing this CBCP:

4.2.2. The IS is inoperable and cannot be recovered within 24 hours.

4.2.3. Key personnel have been identified and trained in their emergency response and recovery roles; they are available to activate this CBCP.

4.2.4. Preventive controls (e.g., generators, environmental controls, waterproof tarps, sprinkler systems, fire extinguishers, and fire department assistance) are fully operational.

4.2.5. IS equipment, including supporting components, are connected to an uninterruptible power supply and generator that provides electricity during a power failure. The generator is serviced by Civil Engineering Squadron (CES) personnel who ensure that the generator does not run short of fuel during generator operations.

4.2.6. IS hardware and software at the original site are unavailable for at least 24 hours.

4.2.7. Current backups of common application software are stored in a General Service Administration (GSA) approved safe located in Building 1100, Unit Manpower and Deployment (UMD) office and are also available for download at **https://cs.eis.af.mil/a6/itrm/default.aspx**.

4.2.8. Current backup of data is located at Building 1090, Medical Group data floor if the Network Area Storage (NAS) is not accessible.

4.2.9. The equipment, connections, and capabilities required to operate the IS are available at the alternate site.

4.2.10. Service agreements are maintained with IS hardware, software, and communications providers to support the emergency recovery operation.

4.2.11. Disaster recovery, continuity of operations, and emergency evacuation procedures are an integral part of this plan.

4.3. Applicable Provisions and Directives

4.3.1. This CBCP complies with the C-E.N.GC.Scott.LittleRock IS contingency planning policy as follows:

4.3.1.1. The organization shall develop a contingency planning capability to meet the needs of supporting operations in the event of a disruption extending beyond 24 hours. The procedures for execution of such a capability shall be documented in a formal CBCP and shall be reviewed at least annually and updated as necessary. Personnel responsible for target systems shall be trained to execute contingency procedures. The plan, recovery capabilities, and personnel shall be tested to identify weaknesses of the capability at least annually.

4.3.1.2. This CBCP also complies with the following federal and departmental policies:

DoDI 8510.01, *DoD Information Assurance Certification and Accreditation Process*

PDD 63, *Critical Infrastructure Protection*

PDD 67, *Enduring Constitutional Government and Continuity of Government Operations*

DoDI 8500.2, *Information Assurance (IA) Implementation*

DoDI 8510.01, *DoD Information Assurance Certification and Accreditation Process*

NIST Special Publication 800-34, *Contingency Planning Guide for Federal Information Systems*

NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*

DoDI 5200.1-R, *Information Security Program*

DoDI 5200.8, *Security of DoD Installations and Resources*

DoDI 5205.02, *DoD Operations Security (OPSEC) Program*

AFI 10-701, *Operations Security (OPSEC)*

AFI 31-401, *Information Security Program Management*

AFI 31-501, *Personnel Security Program Management*

AFI 33-112, *Information Technology Hardware Asset Management*

AFI 33-114, *Software Management*

5. Concept of Operations

5.1. System Descriptions and Architecture

5.1.1. The principal mission of the C-E.N.GC.Scott.LittleRock Information system is to provide real-time command, control, communications, and computer (C4) services for

19AW, 314 AW, 189 ANG AW, USAF Weapon School & 20 other tenants at the worlds premier C-130 Center of Excellence base. The function of the Enterprise is to ensure shared network resources are available 24 hours a day to authorized users within the Non-secure Internet Protocol Router Network (NIPRNet). Enterprise resources consist of all hardware, software, firmware, and facility assets used to support the electronic creation, manipulation, and transfer of information by networked government computers using commercial off-the-shelf (COTS) and Government off-the-shelf (GOTS) developed software.

5.1.2. The Little Rock AFB circuit-enclave is a system comprised of routers, servers, boundary protection/management devices, and desktop clients operating under a single Enterprise Information System Security Policy. This system establishes the circuit-enclave accreditation for the Little Rock AFB Unclassified network. It is associated with the Scott NIPRNet gateway. The CCSDs associated with this circuit enclave are 7H3W, 77BB and 7NP1. There are no GSUs/sub-enclaves associated with this circuit-enclave.

5.1.3. Core enterprise network components and services are operated and maintained by the 561 Network Operations Squadron (NOS). 561 NOS and Little Rock AFB employs the Air Force approved Combat Information Transport System (CITS) Network Management/Network Defense suite to provide network perimeter security.

5.1.4. Enterprise level data security is the responsibility of the 561 NOS, while local data security responsibilities are delegated to the network control center (NCC) associated with Little Rock AFB. The primary site is housed in the NCC located at 988C Cannon Drive, Little Rock AFB, AR.

5.2. Alternate Site

5.2.1. The alternate site is located at Building 112, Little Rock AFB, AR. An AF project is ongoing to install a warm site at the location. The critical core equipment utilized at the alternate site includes1-external/internal switch, 1-external/internal router, 1-firewall, 1-proxy, 1-HBSS server and 1- DHCP. In addition, equipment located in both racks of room 104 will need to be relocated from building 988C to building 112.

5.2.2. If there is a need to standup the alternate site prior to the alternate site project completion, an assessment will be accomplished on the equipment installed in 988C to evaluate operability. If the equipment is usable and the facility event allows, the equipment will be removed and relocated at the alternate site. If the equipment cannot be relocated, the Little Rock NCC will contact 561 NOS to ship the required equipment (DSN: 692-1173, opt 3).

5.2.3. Initial alternate site services will be minimal and confined to critical services only. Web Mail will be used in lieu of Exchange until the Active Directory (ADX) suite is brought online. The Program Office Manager (POM) for GATES, GTIMS, C-130 JMATS and 561 NOS Logging Suite will be responsible for standing up servers at the POM's designated site as documented in service level agreements. 19CS will be responsible for configuring a JET server, a printer server and the backup Network Area Storage (NAS) (located in building 1090). 24 hours of data will be lost when configuring to the backup NAS.

5.3. Interconnections

5.3.1. For all systems that are controlled by a PMO or require special support, there will be a Memorandum of Agreement or a Service Level Agreement signed by the sponsoring organization and the 19 CS/CC. These agreements are maintained in Electronic Records Management (ERM); located at \\ltrvn01\Records\19AW-19MSG-19CS\SCOO and a hardcopy is maintained offsite in building 1100 by the NCC. Attachment 4 lists the interconnection agreements for the C-E.N.GC.Scott.LittleRock.

5.4. Mission Assurance Category (MAC) and Confidentiality Level (CL)

5.4.1. The MAC and CL are described in DoD Instruction 8500.2, Information Assurance Implementation. MAC includes MAC levels I, II, and III. The MAC for Little Rock Enterprise Network (LREN) is MAC II and the CL is sensitive. The IS receives, processes, transmits, stores and/or displays Privacy information, Protected Health Information and Personally Identifiable Information.

5.5. Access Controls

5.5.1. Discretionary access controls are employed when connecting DoD information systems operating at the same classification but with different need-to-know access rules.

5.5.2. When connecting the information systems operating at the same classification level, the system/network administrator configures the router properly using the access control organization's specific router guide so that only authorized services/applications can be transferred from the source to the destination and configure the system software securely to restrict access to system information only to authorized personnel in accordance with DISA Security Technical Implementation Guide (STIG)'s, NSA security guides and organization's specific guides.

5.5.3. When connecting the information systems operating at different classification levels the systems/network administrator explores the type of methods that can be used for cross domain solutions in the system environment and analyze advantages and disadvantages of individual cross domain solutions based on functions and security features. If the system is part of the Global Information Grid (GIG), the system/network administrator installs an National Security Agency (NSA)-developed cross domain solution.

5.5.4. Access is restricted to the Network Control Center (NCC) area as defined by DoD 5200.8-R, Physical Security Program. The room houses the system equipment, and the equipment room has floor-to-ceiling walls. The room is secured within the building by an approved combination door lock. An access list is maintained by the organization security officer and is located at the entrance to the facility. A person with designated escort authorization must escort all visitors.

5.6. Core Software

5.6.1. The Core software in use on the Little Rock Enterprise Network (LREN) enclave is approved for enterprise-wide implementation. Common software such as, Microsoft applications have enterprise-wide licenses and are listed on the AF Infrastructure Technical Reference Model (I-TRM) approved products list (APL) located at: **https://cs.eis.af.mil/a6/itrm/default.aspx**.

5.6.2. Operating systems in use on the network have been identified as the established standard and deemed to be secure when configured correctly. The operating systems in use on this enclave have been tested and approved at the DoD level and local security lockdown procedures are implemented using the appropriate DISA STIG. The Operating Systems in use on this system address object reuse and are designed to clear cache upon logoff thus subsequent users do not have access to the previous user's information.

5.6.3. All software required for recover, following a disaster is stored in a secure location in the NCC. A copy of the software required to support critical missions is also be kept in the off-site storage location in the event that the building is completely destroyed.

5.7. Common Access Kiosks

5.7.1. Specific functions within the 19 AW require common or multi-user access to specific workstations on the network. These systems, commonly referred to as Kiosks, generally require a group account in order for several individuals to have access to workstation applications and/or displays. Currently, Kiosks are employed within the various Flying Training Squadron Operations desks and within the Military Personnel Flight Customer Service section. As a rule, kiosks are approved on a case-by-case basis with rigid scrutiny from the Wing IAO and the NCC. Additionally, maximum security group policy objects (GPO) settings will be employed by the 561 NOS to ensure access is restricted to only those applications and functions specific to the common access requirement.

5.8. Temporary Access

5.8.1. The NCC can provide Local Area Network (LAN) internet access to visiting dignitaries at the Lodging facilities by request. If not requested, access is provided through commercial systems located in the DV suites and hosted by 19 Force Support Squadron (FSS). Distinguished Visitors (DV)'s must register through the 19 AW Protocol Office. The 19 AW/CCP will coordinate and provide the user information to 19 FSS IT personnel.

6. Line of Succession

6.1. An order of succession has been identified, in coordination with management, to ensure that decision-making authority for this CBCP is uninterrupted.

6.2. The Operations Flight Commander is responsible for ensuring the safety of personnel and the execution of procedures documented within this CBCP. If the Operations Flight Commander is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the Deputy Operations Director shall function as that authority. If the Deputy Operations Director is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the Officer In Charge (OIC) of Network Operations shall function as that authority. If the OIC of Network Operations is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the Network Operations Section Chief shall function as that authority. If the Network Operations Section Chief is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the Non-commissioned Officer In Charge (NCOIC) of Network Operations shall function as that authority.

7. Responsibilities

7.1. The following teams have been developed and trained to respond to a contingency event affecting the IS. The CBCP establishes several teams assigned to participate in recovering operations.

7.1.1. The Network Operations Team (NOT) is responsible for recovery of the computer environment and all applications. Members of this team include personnel who are also responsible for the daily operations and system administrative maintenance. The NCOIC of NCC directs the NOT.

7.1.2. The Network Management Team (NMT) is responsible for recovery of the network infrastructure and all associated circuits. Members of this team include personnel who are also responsible for the daily maintenance of network backbone to include Non-Secure Internet Protocol Routing (NIPR) and Secure Internet Protocol Routing (SIPR) hardware, configurations, operating systems, transport medium and system upgrades. The NCOIC of Network Management directs the NMT.

7.1.3. The Damage Assessment Team (DAT) is responsible for accessing the damage of equipment and reporting back to the NOT lead and NMT lead. Members of this team are composed of selected individuals from the Network Operations and Network Management sections based upon experience. The DAT is lead by Network Operations Section Chief

7.2. The relationships of the team leaders involved in IS recovery and their member teams are illustrated in Figure 1 below:

Figure 1. Team Relationships

Cont Plan Coordinator Flt CC/ Deputy Director = Lead Goal = ensure safety of personnel and IS recovery within 24 hours.		
NETOPS Team NCOIC NETOPS = Lead NETOPS Tech = member NETOPS Tech = member Goal = recover system applications and provide administration for critical services	**NETMAN Team** NCOIC NETMAN = Lead NETMAN Tech = member NETMAN Tech = member Goal = recover network infrastructure and establish connection for critical services	**Damage Assessment Team** NET OPS Sec Chief = Lead NETMAN tech = member NETOPS tech = member Goal = quickly assess damage to facilities and equipment. Provide decision makers with accurate information

8. Threats

8.1. The goal in designing this CBCP was to address a means of continuity during or after a major disaster. While each identified threat could result in a disaster by itself, in the case of a major disaster, several of the threats might be present concurrently or occur sequentially, depending on the circumstances.

8.2. It is advisable to develop several levels of strategies that can be applied as needed. For example, a localized fire in the computing center may render some of that space unusable. An appropriate strategy for that event may be temporary relocation of personnel to another office within C-E.N.GC.Scott.LittleRock headquarters or in suitable local office space in another office building or hotel. An event that required temporary evacuation of the computer center such as a truck accident in the tunnel and a chemical spill that may require several days to resolve, may necessitate switchover capabilities and possible regional mirrored redundancy capabilities that would be transparent to the users. An event of greater magnitude, such as an explosion, may render the C-E.E.N.GC.Scott. LittleRock unusable for an extended duration of time and might necessitate a strategy based on mirrored redundancy as well as a secondary strategy involving a commercial "hot site."

8.3. Time sensitivity and mission criticality in conjunction with budgetary limitations, level of threat and degree of risk will be major factors in the development of recommended strategies.

9. Probable Threats

9.1. The following table depicts the threats most likely to impact C-E.N.GC.Scott.LittleRock IS, its components and management. The specific threats that are represented by (X) are considered the most likely to occur within the C-E.N.GC.Scott.LittleRock environment. Sites should adjust accordingly.

Table 2. C-E.N.G.C.Scott.Litle.Rock Risk Analysis Matrix

C-E.N.GC.Scott.LittleRock Risk Analysis Matrix			
Probability of Occurrence:	**High**	**Medium**	**Low**
Air Conditioning Failure		X	
Aircraft Accident			X
Blackmail			X
Bomb Threats			X
Chemical Spills/HazMat			X
Cold/Frost/Snow			X
Communications Loss		X	
Data Destruction		X	
Earthquakes			X
Fire			X
Flooding/Water Damage	X		
Nuclear Mishaps			X
Power Loss/Outage	X		
Sabotage/Terrorism			X
Storms/Tornado	X		
Vandalism/Rioting			X

10. NOTIFICATION AND ACTIVATION PHASE

10.1. This phase of the CBCP addresses the initial actions taken to detect and assess damage inflicted by a disruption to the IS. In an emergency, the top priority is to preserve the health and safety of its staff before proceeding to the Notification and Activation procedures. Based on the assessment of the event, the plan may be activated by the Contingency Planning Coordinator.

10.2. The following notification procedures will be used in the event of a disruption of the IS:

10.2.1. Following a catastrophe, power outage or natural disaster, the on-call technician will report to Building 988 C to assess the situation and attempt to resolve any problems within 24 hours.

10.2.2. As required, the technician will open up a trouble ticket with Owning Agency, (DISA, 561 NOS, etc.). The Owning Agency will remotely resolve the issue or provide guidance on how to resolve the outage. The technician will also contact Communication Focal Point (CFP) at DSN 731-2666 opt 2 to up channel ticket number and current status.

10.2.3. CFP will provide situational awareness to AMC M/ACCC (DSN576-1332).

10.2.4. If the owning agency cannot remotely fix the problem, they will provide guidance. If touch maintenance is required, the on-call technician will make contact with the system administrator of the affected system to resolve the problem.

10.2.5. Once the problem has been resolved the technician will contact the Owning Agency, to close the trouble ticket and notify CFP. The CFP will provide AMC M/ACCC and 19CS leadership with time of closure and fix action.

10.2.6. If the first responder determines that the damage to the building or systems is too extensive, the technician will contact the Contingency Planning Coordinator and report all known information. Contact information for key personnel is located in Attachment 3, Personnel Contact List.

10.2.7. The Contingency Planning Coordinator will notify the systems manager and the Damage Assessment Team Leader and inform them of the event.

10.2.8. The Damage Assessment Team Leader is to begin assessment procedures. The Damage Assessment Team Leader is to notify team members and direct them to complete the assessment procedures outlined in paragraph 10.3 to determine the extent of damage and estimated recovery time.

10.3. Damage Assessment Procedures:

10.3.1. Upon arrival to the site, the Damage Assessment Team will:

10.3.1.1. Check with Fire Department and or Base Civil Engineering prior to entering any damaged structure.

10.3.1.2. Ensure protective equipment is worn to avoid personal injuries.

10.3.1.3. Visually inspect site for any immediate danger (fire, hot electrical wires, trip hazards, structural damage) and take action to prevent personal injury or equipment damage.

10.3.1.4. Assess operability/damage of power system.

10.3.1.5. Assess operability/damage of environmental system.

10.3.1.6. Assess operability/damage of fiber/cabling.

10.3.1.7. Assess operability/damage of equipment.

10.3.1.8. Access network services operability.

10.3.1.9. Report assessment to system manager (if unable to contact report to Contingency Planning Coordinator) to include the current status of network services, assets requiring replacement, assets requiring repair, estimated time of repair or replacement.

10.3.1.10. Team will standby for further instructions.

11. Plan Activation

11.1. The Contingency Planning Coordinator is to evaluate the results and determine whether the CBCP is to be activated and if relocation is required. Based on assessment results, the Contingency Planning Coordinator may need to notify civil emergency personnel (e.g., police, fire) as appropriate.

11.2. The CBCP is to be activated if one or more of the following criteria are met:

11.2.1. The IS will be unavailable for more than 24 hours.

11.2.2. Facility is damaged and will be unavailable for more than 24 Hours.

11.2.3. Request/receive approval from senior management to implement the CBCP.

11.3. If the plan is to be activated, the Contingency Planning Coordinator will take the following steps:

11.3.1. Notify the system manager and all Team Leaders and inform them of the details of the event and if relocation is required. Instruct Team leaders to inform team members of all applicable information and to prepare to respond and relocate as necessary.

11.3.2. Notify remaining personnel on the general status of the incident.

11.3.3. Notify the Alternate site that a contingency event has been declared and personnel/equipment will be relocated.

12. Recovery Operation Phase

12.1. For Server Issues

12.1.1. In the event that a server crashes or becomes unusable it may be necessary to completely rebuild the server from scratch. A software inventory has been completed on every server; it lists all software products loaded on the server. This documentation is maintained in 19 CS/SCOO records drive and a hardcopy will be stored in a GSA approved safe located in Building 1100, UMD office. This inventory includes configuration items as well (i.e. IP address, hostname, etc…) to aid the reconstruction of the server. This inventory is a living document as patches and version upgrades occur it must be updated.

12.1.2. To completely rebuild the server, consult the software inventory for that server and follow the instructions maintained in Network Operations Section, 19 CS/SCOO on loading and configuring software for each server. After the rebuild is complete, consult 561 NOS prior to adding the server back onto the domain. A vulnerability scan (Retina) will need to be conducted to ensure server is added to the domain fully patched and secure.

12.2. For Loss of Power

12.2.1. If damage occurs to Building 988 C that results in a loss of power, the building and network are protected by a generator that will automatically start and provide power for the entire building. All servers, switches and routers are also connected to a facility uninterruptible power supply (UPS). The UPS has the ability to provide power for the equipment until the generator has started and power has stabilized. The UPS will serve as a power regulator and is part of its basic function in the design.

12.2.2. In the case that the generator is damaged or fails to restore power it will be necessary to prepare the network for an orderly shutdown. The shutdown procedures are maintained in the Network Control Center (NCC) standby binder. Following the restoral of commercial power or stabilization of generator power, the network will be prepared for startup. This will be accomplished following the procedures in the NCC standby binder.

12.3. For Flooding

12.3.1. If the building experiences flooding, due to broken water pipes or excess rain, it will be necessary to immediately remove power from the building without regard to any equipment or software damage that may result from a non-orderly shutdown of the network equipment. This will be accomplished by pressing one of three master power shutoffs located on the right hand side of each exit on the server floor.

12.4. For High Temperature

12.4.1. Due to the age of the environmental control units (ECU) it is necessary to consider the maximum operating temperature of the least tolerant network equipment in the server room. Once 95 degrees room temperature has been reached it becomes increasingly important to take steps to lower the temperature by any means necessary. If the ECU is not working properly, 19 CES customer service must be called in order to open a work order for resolution.

12.4.2. The following steps can be taken to reduce the temperature in the server room:

12.4.2.1. Server room doors will be propped open and fans will be used to direct air in a circulating manner to remove the heat from the server room.

12.4.2.2. If the attempts at reducing the temperature are unsuccessful it may become necessary to perform an orderly shutdown of the entire network. This will be accomplished by following the Network Startup and Shutdown procedures in the NCC standby binder.

12.4.2.3. All monitors will be shut off as they are a major heat source. Servers can be remotely shutdown if necessary. Lower priority missions may also be shutdown in

an attempt to lower the room temperature. Priority hardware shutdown is located in the NCC standby binder.

12.5. For Uninhabitable Facility

12.5.1. If building 988C is rendered uninhabitable but the equipment is functional, it will be necessary to relocate personnel resources to an alternate operating location. Our alternate operating location is in building 112. For contingency purposes, we will only relocate personnel and remotely maintain the equipment identified as Critical Resources to support Critical Mission Functions. These functions have been defined as JET, GATES, GTIMS, ASIMS, AHLTA, PACS, ICDB and MPS. Critical resources are defined as equipment necessary to complete or carry on critical mission functions and may be pre-positioned at the alternate operating location to expedite contingency operations in the event of a catastrophe to Building 988C. Critical missions' recovery must be completed within 24hrs with 561 NOS supporting spare part maintenance.

12.6. For Destroyed/Severely Damaged Facility

12.6.1. This section provides procedures for recovering the IS at the alternate site, whereas other efforts are directed to repair damage to the original system and capabilities**.** If building 988C sustains damage that destroys or severely damages the structure and its contents, the critical resources to support scaled down mission critical operations will be established in building 112. The consists of 1-external/internal switch, 1-external/internal router, 1-firewall, 1-proxy, 1-HBSS server and 1-DHCP server. In addition, equipment located in both racks of room 104 will need to be relocated from building 988C to building 112.

12.6.2. The first recovery objective is to restore priority 1 critical core services to the base within 24hrs.

12.6.3. The NETMAN Team will accomplish the first recovery objective by restoring core system connectivity using the following procedures:

12.6.3.1. If feasible remove the following equipment from building 988C: 1-external/internal router, 1- external/internal switch and the equipment located in both racks of room 104. If unable to remove equipment or equipment is not operational, NETOPS will contact 561 NOS to ship new equipment. Once equipment is removed or new equipment is received proceed with 12.6.3.2.

12.6.3.2. Configure and standup external router and connect through secondary SDP at building 536 (circuit 77BB).

12.6.3.3. Configure and standup external switch.

12.6.3.4. Work with NETOPS to standup firewall.

12.6.3.5. Work with NETOPS to standup proxy.

12.6.3.6. Configure and standup internal switch.

12.6.3.7. Work with NETOPS to standup DHCP.

12.6.3.8. Configure and standup internal router.

12.6.3.9. Work with 561 NOS/NETOPS to configure and standup equipment (or replacement equipment) that was located in room 104 of building 988C.

12.6.3.10. Work with NETOPS to standup HBSS.

12.6.3.11. Work with NETOPS to standup Domain Controller.

12.6.4. The NETOPS Team will accomplish the first recovery objective by restoring core system applications (DHCP, firewall, proxy, HBSS, SAN) using the following procedures:

12.6.4.1. If feasible power down and remove the following equipment from building 988C: 1 proxy, 1- firewall, 1- DHCP, 1- Domain Controller and 1- HBSS. If unable to remove equipment or equipment is not operational, contact 561 NOS. to ship new equipment. Once equipment has been relocated proceed with 12.6.4.2.

12.6.4.2. Coordinate with 561 NOS/NETMAN to standup firewall.

12.6.4.3. Coordinate with 561 NOS/NETMAN to standup proxy.

12.6.4.4. Coordinate with 561 NOS/NETMAN to standup DHCP.

12.6.4.5. Coordinate with 561 NOS/NETMAN to standup HBSS.

12.6.4.6. Coordinate with 561 NOS/NETMAN to standup Domain Controller.

12.6.4.7. Notify CFP when core system applications have been restored.

12.6.4.8. Coordinate with Air Force Network Integration Center (AFNIC) to ship new ASIMS (if damaged).

12.6.4.9. Coordinate with 561 NOS to ship a new ADX suite (if damaged).

12.6.4.10. Coordinate with 561 NOS to ship new SCCM suite (if damaged).

12.6.4.11. Coordinate with 561 NOS to ship new retina scanners (if damaged).

12.6.5. The CFP Team will accomplish the first recovery objective by ensuring core system services are established for critical customers using the following procedures:

12.6.5.1. Notify critical customers of network issue and provide ETR.

12.6.5.2. Once minimum services are restored notify critical customers and verify that services/applications are available. If services/applications are not available open a trouble ticket and notify NETMAN/NETOPS/CSC accordingly.

12.6.5.3. Notify base populace that network services are available for critical customers only.

12.6.5.4. As required dispatch client service technicians to repair any computer issues for critical users.

12.6.6. The second recovery objective is to restore priority 1 critical functional information systems to the base within 24hrs. These services include ACES-FD, GATES, GTIMS, AHLTA, JET, ICDB and MPS.

12.6.7. The NETMAN Team will accomplish the second recovery objective by restoring connectivity to critical function systems using the following procedures:

12.6.7.1. Coordinate with NETOPS and route JET server to 536 ITN.

12.6.7.2. Coordinate with 19 LRS and route Gates server data from POM alternate site to most feasible ITN.

12.6.7.3. Coordinate with C-130JMats and route GTIMS data from POM alternate site to most feasible ITN.

12.6.7.4. Coordinate with 29WPS to route servers from POM alternate site through most feasible ITN.

12.6.7.5. Coordinate with Med Gp and route Med Gp circuits from building 1090 to most feasible ITN.

12.6.7.6. Coordinate with NETOPS to route Printer server to 536 ITN.

12.6.7.7. Coordinate with 19 OG to route file server to most feasible ITN.

12.6.7.8. Coordinate with Marine Det to route file server to most feasible ITN.

12.6.8. The NETOPS Team will accomplish the second recovery objective by restoring system applications for critical functional systems using the following procedures:

12.6.8.1. Configure and standup JET server. Work with NETMAN to connect through building 536 ITN.

12.6.8.2. Configure and standup Printer server. Work with NETMAN to connect through building 536 ITN.

12.6.8.3. Configure and standup back up SAN. Once online, notify CFP that SAN is restored but customers may have 24 hr data loss.

12.6.9. The CFP Team will accomplish the second recovery objective by ensuring critical systems are restored to users using the following procedures:

12.6.9.1. Once services are restored (JET, GTIMS, GATES, etc.) notify users.

12.6.9.2. Open trouble tickets and dispatch technicians for any unresolved priority 1 resource issues.

12.6.10. The third recovery objective is to restore priority 2 resources within 72 hours. These resources include ADX Suite, phone servers and GEOBASE.

12.6.11. The NETMAN Team will accomplish the third recovery objective by restoring connectivity to priority 2 resources using the following procedures:

12.6.11.1. Configure AMC router through AMC circuit 7NP1.

12.6.11.2. Work with 561 NOS to route ADX suite through AMC router.

12.6.12. The NETOPS Team will accomplish the third recovery objective by restoring priority 2 system applications using the following procedures:

12.6.12.1. Coordinate with 561 NOS/NETMAN to standup ADX suite.

12.6.12.2. Ensure phone servers are online.

12.6.13. The CFP Team will accomplish the third recovery objective by ensuring priority 2 systems are restored to users utilizing the following procedures:

12.6.13.1. Once services are restored (ADX, GEOBASE, Cons, MXG, FSS) notify users.

12.6.13.2. Open trouble tickets and dispatch technicians for any unresolved priority 2 resource issues.

12.6.14. The fourth recovery objective is to restore priority 3 resources within 1 week.

12.6.15. The NETMAN Team will accomplish the fourth recovery objective by restoring connectivity to priority 3 resources using the following procedure:

12.6.15.1. Work with NETOPA to standup SCCM.

12.6.15.2. Work with NETOPS to standup Retina scanner.

12.6.16. The NETOPS Team will accomplish the fourth recovery objective by restoring priority 3 system applications using the following procedures:

12.6.16.1. Coordinate with 561 NOS/NETMAN to standup SCCM.

12.6.16.2. Coordinate with 561 NOS/NETMAN to standup Retina scanner.

12.6.17. The CFP Team will accomplish the fourth recovery objective by ensuring priority 3 systems are restored to users utilizing the following procedures:

12.6.17.1. Once services are restored notify users.

12.6.17.2. Open trouble tickets and dispatch technicians for any unresolved priority 3 resource issues.

13. Return to Normal Operations

13.1. This section discusses activities necessary for restoring IS operations at the C-E.N.GC.Scott.LittleRock original or new site. When the computer center at the original or new site has been restored, IS operations at the alternate site must be transitioned back. The goal is to provide a seamless transition of operations from the alternate site to the operating facility.

13.2. The NETOPS Team will implement the following procedures to restore IS operations at the original or new site:

13.2.1. Ensure primary critical equipment is operational.

13.2.2. Coordinate ADX suite stand up w/561 NOS Directory Services; test connection to internal router; switch over from Scott AFB domain controllers.

13.2.3. Active SCCM servers in ADX suite; test connection; switch over from alternate site.

13.2.4. Configure DHCP virtual server; test connection; switch over from alternate site.

13.2.5. Transfer HBSS servers from alternate site to primary location; test connection through CITS switch card on internal router; restore service.

13.2.6. Install new Firewall stand up w/561 NOS Boundary Services, test connection through CITS switch card on internal/external router; restore service.

13.2.7. Install new Blue Coat Proxy appliance stand up w/561 NOS Boundary Services; test connection through CITS switch card on internal/external router; restore service.

13.3. The NETMAN Team will implement the following procedures to restore IS operations at the original or new site:

13.3.1. Ensure circuit 7H3W is up and running from building 1100 to building 988C.

13.3.2. Power up SDP equipment, verify good connection to circuit 7H3W.

13.3.3. Connect SDP equipment to External Router.

13.3.4. Connect External Router to Primary/Secondary Firewall.

13.3.5. Connect Primary/Secondary Firewall to Internal Router.

13.3.6. Connect Internal Router to Internal Switch, verify Internal Switch has required connections to ITN 335/ITN 988.

13.4. Neither the NETOPS Team nor the NETMAN Team will have any concurrent processing occurring simultaneously at the original or new site due to the configuration or lack of redundancy of boundary equipment. The system will either be up in its entirety at building 112 or at building 988.

13.5. The NETMAN Team will implement the following procedures in Plan Deactivation:

13.5.1. Reconfigure all ITN routes to load balance with circuit 7H3W, remove 77BB as only circuit in routing.

13.5.2. Deactivate all internal/external routing/switch equipment around circuit 77BB/Bldg 112.

13.6. The NETOPS Team will implement the following procedures in Plan Deactivation:

13.6.1. Remove any spare servers from the network

13.6.2. Reimage and return for cold alt site storage

PATRICK J. RHATIGAN, Col, USAF
Commander, 19th Airlift Wing

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoDI 8510.01, *DoD Information Assurance Certification and Accreditation Process (DIACAP)*, 28 November 2007.

PDD 63, *Critical Infrastructure Protection*, 22 May 1998.

PDD 67, *Enduring Constitutional Government and Continuity of Government Operations*, 21 October 1998.

DoDI 8500.2, *Information Assurance (IA) Implementation*, 6 February 2003.

DoDI 8510.01, *DoD Information Assurance Certification and Accreditation Process (DIACAP),* 28 November 2007.

NIST Special Publication 800-34, *Contingency Planning Guide for Federal Information Systems Revision 1*, May 2010.

NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations Revision 3* August 2009.

DoDI 5200.1-R, *Information Security Program* 24 Feb 2012

DoDI 5200.8, *Security of DoD Installations and Resources* 10 Dec 2005

DoDI 5205.02, *DoD Operations Security (OPSEC) Program* 20 Jun 2012

AFI 10-701, *Operations Security (OPSEC),* 08 Jun 2011

AFI 31-401, *Information Security Program Management*, 01 Nov 2005

AFI 31-501, *Personnel Security Program Management*, 27 Jan 2005

AFI 33-112, *Information Technology Hardware Asset Management*, 07 Jan 2011

AFI 33-114, *Software Management*, 13 May 2004

AFI 33-115v1, *Network Operations (NETOPS),* 24 May 2006

AFI 33-138, *Enterprise Network Operations Notification and Tracking*, 28 Nov 2005

AFI 33-201v1, *Communications Security (COMSEC) (FOUO)*, 01 May 2005

AFI 33-332, *Air Force Privacy Act Program*, 16 May 2011

AFSSI 7702, *Emission Security*

AFSSI 8502, *Organizational Computer Security*

Prescribed Forms

None

Adopted Forms

AF 487 *Emergency Generator Operating Log (Inspection Testing)*

Abbreviations and Acronyms

ADX—Active Directory

AF—Air Force

AFB—Air Force Base

AFNIC—Air Force Network Integration Center

AGFA—Asymptotic Green Function Approximation

AHLTA—Armed Forces Health Longitudinal Technology Application

AIS—Information System Application

AMC—Air Mobility Command

ASIMS—Automated Security Incident Measurement System

CBCP—Contingency and Business Continuity Plan

CES—Civil Engineering Squadron

CFP—Communications Focal Point

CHCS—Composite Health Care System

CITS—Combat Information Transportation System

CL—Confidentiality Level

COTS—Commercial Off-The-Shelf

CSC—Client Service Center

DAT—Damage Assessment Team

DDRS—Digital Dental Radiography Solution

DHCP—Dynamic Host Configuration Protocol

DISA—Defense Information Systems Agency

DOD—Department of Defense

DMLSS—Defense Medical Logistics Standard Support

DNS—Domain Name System

ECU—Environmental Control Unit

ETR—Estimated Time of Repair

FSS—Force Support Squad

GATES—Global Air Transportation Execution System

GOTS—Government Off-The-Shelf

GSL—General Sales License

GTIMS—Graduate Training Integration Management System

HBSS—Host Base Security System

HVAC—Heating, Ventilation and Air Conditioning

IAO—Information Assurance Officer

ICDB—Integrated Clinical Database

IS—Information System

IT—Information Technology

ITN—Information Transfer Node

I-TRM—Infrastructure Technical Reference Number

JET—Joint Environmental Toolset

LREN—Little Rock Enterprise Network

MAC—Mission Assurance Category

MPS—Mission Planning System

MXG—Maintenance Group

NAS—Network Area Storage

NCC—Network Control Center

NCOIC—Non-commissioned Officer In Charge

NETMAN—Network Maintenance

NETOPS—Network Operations

NIPR—Non-secure Internet Protocol Routing

NOS—Network Operations Squadron

NOT—Network Operations Team

NMT—Network Management Team

OG—Operations Group

OIC—Officer In Charge

OPR—Office of Primary Responsibility

PACS—Picture Archiving and Communication System

POM—Program Office Manager

SAN—Storage Area Network

SCCM—System Center Configuration Manager

SDP—Secondary Distribution Point

SIPR—Secure Internet Protocol Routing

STIG—Security Technical Implementation Guide

UPS—Uninterruptible Power Supply

VPN—Virtual Private Network

Attachment 2

CONTACT LIST

Contact LIST		
Title	**Point of Contact**	**Phone No.**
CFP	19CS/SCOS	W:987-2666 M:425-7286
AMC M/ACCC	Shift Leader	DSN:576-1332
19 CS Commander	19CS/CC	W:987-3735 M:313-7264
19 AW Command Post	19AW/CP	987-1900
561 NOS	Shift Leader	DSN:692-1178 opt 3
Contingency Plan Coordinator	SCO Flight Commander	W: 987-6410 M: 765-7647
Contingency Plan Coordinator Alternate	Deputy Operations Director	W: 987-7743
System Manager	Deputy Operations Director	W: 987-7743
System Manager Alternate	OIC Network Ops	W:987-6596
Damage Assessment Team Lead	Network Ops Sec Chief	W:987-6596 M: 442-7402
Damage Assessment Team Lead Alternate	NCOIC NETMAN	W:987-2900 M: 442-7402
NETOPS Team Members	NETOPS Techs	W:987-5500 M:366-0805
NETMAN Team Members	NETMAN Techs	W:987-2900 M:425-5577
Damage Assessment Team Members	NETMAN/NETOPS Techs	NeTMaN :987-2900 NetMan: 442-7402 NetOps:987-5500 NetOps:366-0805

Attachment 3

FSA/VENDOR LIST

FSA/VENDOR LIST			
Title	**Point of Contact**	**Contact number**	**E-mail**
19MDG (FSA)	Vida Waters Scott Messner	W:987-8057 W:987-7263	P:vida.waters@us.af.mil A:scott.messner@us.af.mil
19 FSS (FSA)	Sean Donohoe	W:987-7840	P:sean.donohoe@us.af.mil
19 CONS (FSA)	Gary Price Jane Utley	W:987-2054	P:gary.price.5@us.af.mil A:jane.utley@us.af.mil
19 LRS (FSA)	Raymond Altes Joshua Stewart, SSgt (Fuels)	W:987-3047 W:987-5522	P:Raymond.altes@us.af.mil A:joshua.stewart.9@us.af.mil
19 CES (FSA)	Frank Jordan	W:987-7542	P:frank.jordan@us.af.mil
C-130 JMATS (FSA)	Keith Jones John Bensen Toby Tucker	W:987-5150 x280 W:987-5150 x279 W:987-5150 x210	P:keith.jones.27.ctr@us.af.mil A:john.bensen.ctr@us.af.mil A:toby.tucker.1.ctr@us.af.mil
 (UPS Maint)	JT Packard	W:800-972-9778	W:
T-Metrics	Aaron Vonderharr, SSgt	W:987-2900	P:aaron.vonderharr@us.af.mil
E-911	Aaron Vonderharr, SSgt	W:987-2900	P:aaron.vonderharr@us.af.mil
ETOV	Sharon Smith (19th AW) Patrick Fulks (314th AW)	W:987-7085 W: 987- 8879	P:Sharon.smith.2.ctr@us.af.mil P:Patrick.fulks.ctr@us.af.mil
314th AW MPS	Darrel Fenton	W:987-2071	P:Darrel.fenton@us.af.mil
19th AW MPS	Darin Dykes Russall Sawyer	W:987-3995 W:987-6229	P:darin.dykes.ctr@us.af.mil A:Russell.sawyer.4.ctr@us.af.mil
GATES	Michael Bonecutter, TSgt	W:987-3328	P:michael.bonecutter@us.af.mil
29WPS	Ken Coleman Danielle Harvey, SSgt	W:987-8427 W:987-5255	kenneth.coleman.3@us.af.mil danielle.harvey.3@us.af.mil

Attachment 4

CONTRACTS AND/OR AGREEMENTS

CONTRACTS AND/OR AGREEMENTS	
CURRENT NIPR SYSTEM INTERCONNECT AGREEMENTS	EFFECTIVE DATE
19th Medical Dental Group	1 Apr 08
19 CES – ACES-FD Service Level Agreement	1 Apr 08
19 CONS – SPS Service Level Agreement	1 Apr 08
Lockheed Martin (C130J MATS)	25 Jan 13
GATES	22 Mar 10
GTIMS	1 Apr 08
29 WPS	1 Apr 08
19AW Mission Planning Systems (MPS)	ATO on file with WIA
314 AW Mission Planning Systems (MPS)	ATO on file with WIA
AETC Geospatial Library (GPL)	13 Mar 06
ETOV	1 Apr 08

Attachment 5

PRIORITY RECOVERY

A5.1. The following table lists the resources and their recovery time based upon a business analyses of LRAFB mission requirements. Priority 1 resources have been determined to cause mission failure if the systems are not restored within 24 hours. Priority 2 resources have been determined to cause mission degradation if the systems are not restored within 72 hours. Priority 3 resources have been determined to cause mission degradation if the resources are not restored within one week.

PRIORITY RECOVERY				
PRI	**RESOURCE/ IP ADDRESS**	**CUSTOMER**	**DEVICE NAME**	**LOCATION**
1	SDP Switch	AFNET/ DSN: 692-6672		BLD 1100
1	SDP Router	AFNET/ DSN: 692-6672		BLD 1100
1	External Router	INOSC-W		Building 988c NCC
1	Ext Switch	INOSC-W		Building 988c NCC
1	Firewall	INOSC-W		Building 988c NCC
1	Proxy	INOSC-W		Building 988c NCC
1	Internal Switch	INOSC-W		Building 988c NCC
1	Internal Router	INOSC-W		Building 988c NCC
1	DHCP/ 137.3.240.201	AFNET/ DSN: 692-6672	52NKAK-HC-001v	Building 988c NCC
1	Domain Controller/ 137.3.240.183	AFNET/ DSN: 692-6672	52NKAK-DC-001	Building 988c NCC
1	ASIMS	AFNET/ DSN: 692-6672		
1	HBSS	AFNET/ DSN: 692-6672	52NKAK-AV-001v	Building 988c NCC
1	CORE ITN	NETMAN/DSN:731-2500		Building 988c NCC
1	CORE ITN	NETMAN/ DSN:731-2500		BLD 335
1	ITN	NETMAN/ DSN:731-2500		BLD 536
1	ITN	NETMAN/ DSN:731-2500		BLD 1250
1	ITN	NETMAN/ DSN:731-2500		BLD 370
1	ITN	NETMAN/ DSN:731-2500		BLD 350
1	ITN	NETMAN/ DSN:731-2500		BLD 314
1	VPN Concentrator 137.3.122.37			Building 988c NCC
1	JET/ 137.3.254.181	NCC	LTRPR05003	Building 988c NCC
1	JET	NCC		Building 988c NCC
1	File Server/ 137.3.254.44	JMATS/ DSN: 731-5150	LTRAP044	Building 988c NCC
1	File Server/ 137.3.254.51	JMATS/ DSN: 731-5150	ltrap051	Building 988c NCC
1	File Server/Database Server/ 137.3.254.83	JMATS/ DSN: 731-5150	LTRFS083	Building 988c NCC
1	File Server/ 137.3.254.44	JMATS/ DSN: 731-5150	LTRAP044	Building 988c NCC
1	GTIMS Web Server/ 137.3.254.50	JMATS/ DSN: 731-5150	LTRWS050	Building 988c NCC
1	GTIMS Web Server/ 137.3.254.117	JMATS/ DSN: 731-5150	ltrws117	Building 988c NCC
1	GTIMS Database Server/ 137.3.254.112	JMATS/ DSN: 731-5150	ltrdb121	Building 988c NCC
1	LCMS Database Server/ 137.3.254.116	JMATS/ DSN: 731-5150	ltrdb116	Building 988c NCC
1	GTIMS	JMATS/ DSN: 731		Building 988c NCC

PRI	RESOURCE/ IP ADDRESS	CUSTOMER	DEVICE NAME	LOCATION
1	GTIMS	JMATS/ DSN: 731		Building 988c NCC
1	GTIMS	JMATS/ DSN: 731		Building 988c NCC
1	NEW PEX/ 137.3.254.113		LTRPEX01	Building 988c NCC
1	FILE SERVER/ 137.3.254.52	29 WPS/ DSN: 731-8427	LTRAP06703	Building 988c NCC
1	FILE SERVER/ 137.3.254.93	29 WPS/ DSN: 731-8427	LTRAP10403	Building 988c NCC
1	GATES Server/ 137.3.254.110	19 LRS/ DSN: 731-7127	LTRAP22203	Building 988c NCC
1	Fuels server/ 137.3.52.55	19LRS/ DSN: 731-3016	LTRAP11103	Building 295
1	19 LRS Server/ 137.3.198.16	19 LRS/ DSN: 731-3016	LTRAP11203	Building 1342
1	ASIMS/ 137.3.32.006	19MDG/ DSN: 731-8057	LTRSQL006P2	Building 1090
1	AHLTA Pri/ 137.3.32.130	19MDG/ DSN: 731-8057	SERVER AHLTA PRIMARY	Building 1090
1	DDRS/ 137.3.32.008	19MDG/ DSN: 731-7263	LTRDDRS008P2	Building 1090
1	AHLTA/ 137.3.32.131	19MDG/ DSN: 731-8057	TIVOLI SERVER	Building 1090
1	PACS/ 137.3.35.40	19MDG/ DSN: 731-8057	LTRDB040P2	Building 1090
1	ICDB DATABASE SERVER/ 137.3.32.126	19MDG/ DSN: 731-8057	FS-MDGICDB	Building 1090
1	GSL-PHARMACY/ 137.3.32.35	19MDG/ DSN: 731-7263	52NKAK-SS-901	Building 1090
1	AHLTA LCS Secondary/ N/A	19 MDG/ DSN: 731-8057	SERVER AHLTA SECONDARY	Building 1090
1	CHCS Node A (Medical Records, Lab, etc)/ 137.3.32.010	19 MDG/ DSN: 731-8057	SERVER - NODE A	Building 1090
1	CHCS Node A (Medical Records, Lab, etc)/ 137.3.32.011	19 MDG/ DSN: 731-8057	SERVER - NODE B	Building 1090
1	CHCS/ 137.3.32.016	19 MDG/ DSN: 731-8057	STORAGE WORKS	Building 1090
1	DII 1 -- part of AHLTA/ 137.3.32.012	19 MDG/ DSN: 731-8057	DII SERVER - PRIMARY	Building 1090
1	DII II -- part of AHLTA/ 137.3.32.018	19 MDG/ DSN: 731-8057	DII SERVER - SECONDARY	Building 1090
1	SAM - part of AHLTA/ 137.3.32.013	19 MDG/ DSN: 731-8057	SAM SERVER	Building 1090
1	ICDB Interface Server - part of CHCS/ 137.3.32.127	19 MDG/ DSN: 731-8057	FS-MDGICDBIS	Building 1090
1	ICDB Web Server -- part of CHCS/ 137.3.32.128	19 MDG/ DSN: 731-8057	FS-MDGICDBWEB	Building 1090
1	HDM-CCE on BladeFrame (Coding Compliance Editor)/ 137.3.32.136	19 MDG/ DSN: 731-8057	LTRGA136P2	Building 1090
1	Comm - CCE on BladeFrame/ 137.3.32.137	19 MDG/ DSN: 731-8057	LTRGA137P2	Building 1090
1	PACS (Application Server) - Digital Radiology/ 137.3.35.41	19 MDG/ DSN: 731-8057	LTRAPP041P2	Building 1090
1	PACS (Connectivity Mgr) – Digital Radiology/ 137.3.35.42	19 MDG/ DSN: 731-8057	LTRCM042P2	Building 1090
1	PACS (IMPAX Digital Radiology) SMMS Server/ 137.3.35.43	19 MDG/ DSN: 731-8057	LTRSMMS043P2	Building 1090
1	PACS (SAN/Filer) - Dig Radiology / 137.3.35.44/45	19 MDG/ DSN: 731-8057	LTRCACHE044P2	Building 1090
1	Archive of Digital x-rays/ 137.3.35.46	19 MDG/ DSN: 731-8057	LTRUDO046P2	Building 1090

PR	RESOURCE/ IP ADDRESS	CUSTOMER	DEVICE NAME	LOCATION
1	AGFA - Proxy server - Dig Radiology/ 137.3.35.61/62	19 MDG/ DSN: 731-8057	52NKAKSS900	Building 1090
1	E2569 Server -- Third Party Collections Server/ 137.3.32.40	19 MDG/ DSN: 731-8057	52NKAK-FS-01	Building 1090
1	TOL Server - Blade (tricare online)/ 137.3.32.123	19 MDG/ DSN: 731-8057	FS-MDGTOL1	Building 1090
1	BOBJ Server – Blade/ 137.3.32.124	19 MDG/ DSN: 731-8057	B-0013	Building 1090
1	SQL Server -- internal database, KIOSK/ 137.3.32.120	19 MDG/ DSN: 731-8057	FS-MDGSQL	Building 1090
1	NETAPP CLUSTER SERVER - SAN FILE SERVER/ 137.3.32.132	19 MDG/ DSN: 731-8057	LTRFS132P2	Building 1090
1	NETAPP CLUSTER SERVER - SAN FILE SERVER/ 137.3.32.133	19 MDG/ DSN: 731-8057	LTRFS133P2	Building 1090
1	DMLSS Server - Logistics Ordering/ 214.2.227.4	19 MDG/ DSN: 731-8057	AMEDNKAK0A0C4	Building 1090
1	GSL -- Pharmacy -- drug dispense cabinets/ 137.3.32.36	19 MDG/ DSN: 731-8057	52NKAK-SS-902	Building 1090
1	ACES-FD	19 CES/ DSN: 731-7542	ltracesfd03103	Building 239
1	PRINT SERVER/ 137.3.254.137	NCC	LTRPR05003	Building 988c NCC
1	Marine File Server/ 137.3.254.60	NCC	LTRFS05	Building 988c NCC
1	File Server/ 137.3.254.130	314 OG/ DSN: 731-6423	LTRAP13003	Building 988c NCC
1	File Server/ Unknown	314 OG/ DSN: 731-6423	52NKAK-FS-001	Building 988c NCC
2	SDP Router (77BB)	NETMAN/ DSN:731-2500	N/A	BLD 536
2	AMC Router			Building 988c NCC
2	ADX suite			Building 988c NCC
2	Phone Server/ 137.3.7.205	NETMAN/ DSN:731-2500	LTRAP55703	Building 335
2	Phone Server/ 137.3.7.206	NETMAN/ DSN:731-2500	LTRAP55603	Building 335
2	Phone Server/ 137.3.7.208	NETMAN/ DSN:731-2500	LTRAP55503	Building 335
2	Phone Server/ 137.3.7.222	NETMAN/ DSN:731-2500	52NKAK-VMS-M9Q1	Building 335
2	Phone Server/ 137.3.7.252	NETMAN/ DSN:731-2500	LTRAP10003	Building 335
2	GEOBASE/ 137.3.116.107	19 CES/ DSN: 731-7542	LTRAP16003	Building 536
2	GEOBASE/ 137.3.116.75	19 CES/ DSN: 731-7542	LTRAP11403	Building 536
2	File Server/ 137.3.116.112	19 CES/ DSN: 731-7542	LTRFS11203	Building 536
2	File Server/ 137.3.116.31	19 CES/ DSN: 731-7542	LTRFS16603	Building 536
2	File Server/ 137.3.116.33	19 CES/ DSN: 731-7542	LTRFS03603	Building 536
2	File Server/ 137.3.116.40	19 CES/ DSN: 731-7542	LTRAP04603	Building 536
2	File Server/ 137.3.116.71	19 CES/ DSN: 731-7542	LTRAP04703	Building 536
2	File Server/ 137.3.116.73	19 CES/ DSN: 731-7542	LTRFS11003	Building 536
2	File Server/ 137.3.116.74	19 CES/ DSN: 731-7542	ltrfs11103	Building 536
2	Backup Server/ 137.3.116.34	19 CES/ DSN: 731-7542	LTRBU10403	Building 536
2	Backup Server/ 137.3.116.113	19 CES/ DSN: 731-7542	LTRBU11303	Building 536
2	NCC SAN/ 137.3.254.81	NCC	ltr-r200	Building 988c NCC
2	Application/Database Server/ 137.3.124.11	19 CONS/ DSN: 731-2054	52NKAK-AS-002	Building 642
2	Application Server/ 137.3.124.12	19 CONS/ DSN: 731-2054	52NKAK-AS-003	Building 642

PRI	RESOURCE/ IP ADDRESS	CUSTOMER	DEVICE NAME	LOCATION
2	File Server/ 137.3.124.23	19 CONS/ DSN: 731-2054	LTRFS02303	Building 642
2	SQL Server/ 137.3.231.53	19 MXG/ DSN: 731-5041	LTRAP01603	Building 276
2	Backup Server/ 137.3.231.102	19 MXG/ DSN: 731-5041	52NKAK-BS-703	Building 276
2	Sign-In Server/ 137.3.216.146	19 FSS/ DSN: 731-3188	LTRAP145	Building 1255
3	Print Server/ 137.3.254.49	NCC	ltrpr04903	Building 988c NCC
3	Print Server/ Unknown	AFNET/ DSN: 692-6672	52NKAK-QS-001v	Building 988c NCC
3	SCCM/ 137.3.240.184	AFNET/ DSN: 692-6672	52NKAK-CM-001	Building 988c NCC
3	SCCM/ 137.3.240.185	AFNET/ DSN: 692-6672	52NKAK-CM-002	Building 988c NCC
3	SCCM/ 137.3.240.187	AFNET/ DSN: 692-6672	52NKAK-CM-003	Building 988c NCC
3	SCCM/ 137.3.240.196	AFNET/ DSN: 692-6672	52NKAK-CM-004v	Building 988c NCC
3	SCCM/ 137.3.240.197	AFNET/ DSN: 692-6672	52NKAK-CM-005v	Building 988c NCC
3	SCCM/ 137.3.240.205	AFNET/ DSN: 692-6672	52NKAK-CM-006v	Building 988c NCC
3	SCCM/ 137.3.240.206	AFNET/ DSN: 692-6672	52NKAK-CM-007v	Building 988c NCC
3	Smarts/ 137.3.200.20	AFNET/ DSN: 692-6672	52NKAK-SMA-001	Building 988c NCC
3	NETMAN Ciscoworks/ 137.3.123.50	NCC	LTRCW01	Building 988c NCC
3	Retina Server/ 137.3.254.113	NCC	LTRAP00303	Building 988c NCC
3	Retina Server/ 137.3.254.119	NCC	LTRAP00203	Building 988c NCC
3	Retina Server/ 137.3.254.36	NCC	LTRAUDIT02	Building 988c NCC
3	Retina Server/ 137.3.254.56	NCC	LTRAP00103	Building 988c NCC
3	Retina Server/ 137.3.254.58	NCC	LTRAUDIT01	Building 988c NCC
3	DHCP/ 137.3.240.201	AFNET/ DSN: 692-6672	52NKAK-HC-001v	Building 988c NCC
3	DHCP/ 137.3.240.201	AFNET/ DSN: 692-6672	52NKAK-HC-001v	Building 988c NCC
3	DHCP/ 137.3.240.202	AFNET/ DSN: 692-6672	52NKAK-TS-002v	Building 988c NCC
3	DHCP/ 137.3.240.202	AFNET/ DSN: 692-6672	52NKAK-TS-002v	Building 988c NCC
3	Domain Controller/ 137.3.240.186	AFNET/ DSN: 692-6672	52NKAK-DC-002	Building 988c NCC
3	Domain Controller/ 137.3.240.186	AFNET/ DSN: 692-6672	52NKAK-DC-002	Building 988c NCC
3	File Server Cluster/ 137.3.254.11	NCC	LTRCL01	Building 988c NCC
3	File Server/ 137.3.254.34	NCC	LTRFS01	Building 988c NCC
3	File Server/ 137.3.254.35	NCC	LTRFS02	Building 988c NCC
3	File Server/ 137.3.254.41	NCC	LTRFS07	Building 988c NCC
3	File Server/ 137.3.254.42	NCC	LTRFS06	Building 988c NCC
3	File Server Virtual Node/ 137.3.254.45	NCC	LTRVN01	Building 988c NCC
3	Backup SAN/ Unknown	NCC	52NKAK-SM-001	Building 988c NCC
3	Backup Server/ 137.3.254.20	NCC	ltrbu01	Building 988c NCC
3	Backup Server/ 137.3.240.182	AFNET/ DSN: 692-6672	52NKAK-BS-001	Building 988c NCC